IN THE CLAIMS

1. (Currently Amended) A real-time reference monitor software product comprising, on a machine-readable medium, a sequence of instructions defining:

a storage area where real-time state information is stored and from which the state information is restored;

a plurality of rules defining allowable activity based on a pattern of activity; and

plural interceptors identifying and governing the activity by selectively computing a decision to allow or block activity based on an application of the rules to the activity;

a process which correlates the state information across different ones of the plural interceptors;

the process which correlates the state information further comprising:

a rule which defines permissible resource references in view of activity identified by the interceptors and the state information, the interceptors operable to receive a sequence of events indicative of requests for operating system resources; and

a rule interpreter which applies the rule to the activity identified and the state information.

2. Canceled

3. (Currently Amended) The software product of claim ~~2~~1, wherein at least one of the plural interceptors is a pre-existing element of a conventional computer operating system.

4. (Currently Amended) The software product of claim ~~2~~1, wherein the process which correlates the state information further comprises:

a rule which defines permissible resource references in view of activity identified by the interceptors and the state information, the rules defining a processing policy; ~~and~~

a rule interpreter which applies the rule to the activity identified and the state information; and

stateful reference monitor operable to compute a decision based on the processing policy to block or allow the event to be transmitted.

5. (Original) The software product of claim 4, wherein the rule can be modified without restarting the real-time reference monitor.

6. (Original) The software product of claim 5, wherein the storage area has contents which are preserved when the rule is modified.

7. (Original) The software product of claim 1, wherein the plural reference interceptors correspond to more than one resource type and wherein the storage area is a single storage area.

8. (Original) The software product of claim 1, further comprising:
an application program interface that can send messages to application programs on the same system.

9. (Original) The software product of claim 8, further comprising:
an application program interface that can send messages to application programs on other systems.

10. (Original) The software product of claim 1, wherein the plural reference interceptors monitor two or more of file access, registry access, network access, object access, system call access, keyboard access, external inputs and user input.

11. (Currently Amended) A computer-implemented reference monitor, comprising:

a monitoring process, executing on a computer, which detects plural defined events and generate event messages;

a storage device, on the computer, in which is stored information related to the event messages generated by the monitoring process; and

a rule interpreting process, executing on the computer, which responds to characteristics of an event message of the information stored in the storage device and a set of rules by modifying operation of the computer by selectively computing a decision to allow or block activity according to the set of rules, the rule interpreting process further comprising:

at least one rule which defines permissible resource references in view of activity identified by the interceptors and the state information, the interceptors operable to receive a sequence of events indicative of requests for operating system resources, the set of rules collectively defining a processing policy; and

a rule interpreter which applies the rule to the activity identified and the state information.

12. (Original) The computer-implemented reference monitor of claim 11, wherein the set of rules is modified in response to the information stored in the storage device.

13. (Original) The computer-implemented reference monitor of claim 12, wherein the set of rules is modified and wherein the information stored in the storage device is preserved when the set of rules is modified.

14. (Original) The computer-implemented reference monitor of claim 11, further comprising an external event message generating process executing on another computer, wherein the external event message generating process communicates event messages to the rule interpreting process.

Claims 15-19. (Canceled)

20. (Currently Amended) The software product of claim 1~~19~~, wherein the plural reference interceptors correspond to more than one resource type and wherein the storage area is a single storage area responsive to a stateful reference monitor for

computing a processing policy decision based on a state determined from the events from the plural reference interceptors, the plural interceptors are operable to monitor at least two of file access, registry access, network access, object access, system call access, keyboard access, external inputs and user inputs.

21. (New) The method of claim 11 wherein stateful reference monitor computes a decision based on the processing policy defined by the rules to block or allow the event to be transmitted.

22. (New) The method of claim 21 wherein the rules further comprise compiled rule byte code operable to perform selection of an active rule set and an inactive rule set such that only a particular rule set is in effect at a particular time.

23. (New) The method of claim 22 wherein the stateful reference monitor is further operable to overwrite the rule byte code in a predetermined memory area and overwriting revised result byte code to effect a revised active rule set; the rule set operable for dynamic modification during persistent system operation.

24. (New) The method of claim 23 wherein the rules defining allowable and disallowable activity further comprise a predetermined pattern of events and an identified prohibited pattern.

25. (New) The method of claim 24 wherein the stateful reference monitor is further operable to:

operate in a state collection mode, the state collection mode operable for gathering normal patterns of activity;

subsequently operate in a lockdown mode, the lockdown mode operable to detect and distinguish predetermined patterns of events and the gathered normal patterns of activity; and

identify detected patterns as unsafe based on user selection.

26. (New) An encoded set of processor based instructions on a machine-readable medium for performing a method of event processing employing a real-time stateful reference monitor including:

a set of instructions defining a storage area where real-time state information is stored and from which the state information is restored;

a set of instructions including a plurality of rules defining allowable activity based on a pattern of activity; and plural interceptors identifying and governing the activity by selectively computing a decision to allow or block activity based on an application of the rules to the activity;

a set of instructions for correlating the state information across different ones of the plural interceptors, the process including the set of instructions which correlates the state information further comprising:

a rule which defines permissible resource references in view of activity identified by the interceptors and the state information, the interceptors operable to receive a sequence of events indicative of requests for operating system resources; and

a rule interpreter which applies the rule to the activity identified and the state information;

a set of instructions for computing a decision based on the processing policy defined by the rules to block or allow the event to be transmitted, the rules further comprising compiled rule byte code operable to perform selection of an active rule set and an inactive rule set such that only a particular rule set is in effect at a particular time, the rules defining allowable and disallowable activity further comprising a predetermined pattern of events and an identified prohibited pattern;

the set of instructions defining the identified prohibited pattern further comprising:

a set of instructions for operating in a state collection mode, the state collection mode operable for gathering normal patterns of activity;

a set of instructions for subsequently operating in a lockdown mode, the lockdown mode operable to detect and distinguish predetermined patterns of events and the gathered normal patterns of activity; and

a set of instructions for identifying detected patterns as unsafe based on user selection.